COUNCIL OF THE EUROPEAN UNION

Brussels, 9 July 2013

11680/13

Interinstitutional File: 2010/0273 (COD)

CODEC 1628
DROIPEN 84
TELECOM 185
PE 323

INFORMATION NOTE

from:	General Secretariat
to:	Permanent Representatives Committee/Council
Subject:	Proposal for a Directive of the European Parliament and of the Council on attacks against information systems and repealing Council Framework Decision 2005/222/JHA - Outcome of the European Parliament's first reading (Strasbourg, 1 to 4 July 2013)

I. INTRODUCTION

In accordance with the provisions of Article 294 of the TFEU and the joint declaration on practical arrangements for the codecision procedure [1], a number of informal contacts have taken place between the Council, the European Parliament and the Commission with a view to reaching an agreement on this dossier at first reading, thereby avoiding the need for second reading and conciliation.

In this context, the rapporteur, Mrs Monika HOHLMEIER (EPP-DE) presented one compromise amendment to the proposal for Directive, on behalf of the Committee on Civil Liberties, Justice and Home Affairs. This amendment had been agreed during the informal contacts referred to above.

[1] OJ C 145, 30.6.2007, p. 5.

II. VOTE

When it voted on 4 July 2013, the plenary adopted the compromise amendment to the proposal for a Directive. The Commission's proposal as thus amended and the legislative resolution constitute the European Parliament's position at first reading; it reflects what had been previously agreed between the institutions. The Council should therefore be in a position to approve the position of the European Parliament. The legislative act would then be adopted in the wording which corresponds to this position.

The text of the amendment adopted and the European Parliament's legislative resolution are set out in the Annex. The amendment is presented in the form of a consolidated text, where changes to the Commission's proposal are highlighted in ***bold and italics***. The symbol "▌" indicates deleted text.

Attacks against information systems ***I

European Parliament legislative resolution of 4 July 2013 on the proposal for a directive of the European Parliament and of the Council on attacks against information systems and repealing Council Framework Decision 2005/222/JHA (COM(2010)0517 – C7-0293/2010 – 2010/0273(COD))

(Ordinary legislative procedure: first reading)

The European Parliament,

– having regard to the Commission proposal to Parliament and the Council (COM(2010)0517),

– having regard to Article 294(2) and Article 83(1) of the Treaty on the Functioning of the European Union, pursuant to which the Commission submitted the proposal to Parliament (C7-0293/2010),

– having regard to Article 294(3) of the Treaty on the Functioning of the European Union,

– having regard to the opinion of the European Economic and Social Committee of 4 May 2011[1],

– having regard to the undertaking given by the Council representative by letter of 21 June 2013 to approve Parliament's position, in accordance with Article 294(4) of the Treaty on the Functioning of the European Union,

– having regard to Rule 55 of its Rules of Procedure,

– having regard to the report of the Committee on Civil Liberties, Justice and Home Affairs and the opinions of the Committee on Foreign Affairs and the Committee on Industry, Research and Energy (A7-0224/2013),

1. Adopts its position at first reading hereinafter set out;

2. Calls on the Commission to refer the matter to Parliament again if it intends to amend its proposal substantially or replace it with another text;

3. Instructs its President to forward its position to the Council, the Commission and the national parliaments.

[1] OJ C 218, 23.7.2011, p. 130.

P7_TC1-COD(2010)0273

Position of the European Parliament adopted at first reading on 4 July 2013 with a view to the adoption of Directive 2013/.../EU of the European Parliament and of the Council on attacks against information systems and *replacing* Council Framework Decision 2005/222/JHA

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 83(1) thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Economic and Social Committee[1],

Acting in accordance with the ordinary legislative procedure[2],

[1] OJ C 218, 23.7.2011, p. 130.

[2] Position of the European Parliament of 4 July 2013.

Whereas:

(1) The objectives of this Directive are to approximate ***the criminal law*** of the Member States in the area of attacks against information systems ***by establishing minimum rules concerning the definition of criminal offences and the relevant sanctions*** and to improve cooperation between ▌ competent authorities, including the police and other specialised law enforcement services of the Member States***, as well as the competent specialised Union agencies and bodies, such as Eurojust, Europol and its European Cyber Crime Centre, and the European Network and Information Security Agency (ENISA).***

(2) Information systems are a key element of political, social and economic interaction in the Union. Society is highly and increasingly dependent on such systems. The smooth operation and security of those systems in the Union is vital for the development of the internal market and of a competitive and innovative economy. Ensuring an appropriate level of protection of information systems should form part of an effective comprehensive framework of prevention measures accompanying criminal law responses to cybercrime.

(3) Attacks against information systems, and, in particular, ***attacks linked to*** organised crime, are a growing menace ***in the Union and globally***, and there is increasing concern about the potential for terrorist or politically motivated attacks against information systems which form part of the critical infrastructure of Member States and of the Union. This constitutes a threat to the achievement of a safer information society and of an area of freedom, security***,*** and justice, and therefore requires a response at Union level ***and improved cooperation and coordination at international level***.

(4) There are a number of critical infrastructures in the Union, the disruption or destruction of which would have a significant cross-border impact. It has become apparent from the need to increase the critical infrastructure protection capability in the Union that the measures against cyber attacks should be complemented by stringent criminal penalties reflecting the gravity of such attacks. Critical infrastructure could be understood to be an asset, system or part thereof located in Member States, which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, such as power plants, transport networks or government networks, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions.

(5) There is evidence of a tendency towards increasingly dangerous and recurrent large-scale attacks conducted against information systems which ***can often be*** critical to Member States or to particular functions in the public or private sector. This tendency is accompanied by the development of increasingly sophisticated ***methods, such as the creation and use of so-called "botnets", which involves several stages of a criminal act, where each stage alone could pose a serious risk to public interests. This Directive aims, inter alia, to introduce criminal penalties for the creation of botnets, namely, the act of establishing remote control over a significant number of computers by infecting them with malicious software through targeted cyber attacks. Once created, the infected network of computers that constitute the botnet can be activated without the computer users' knowledge in order to launch a large-scale cyber attack, which usually has the capacity to cause serious damage, as referred to in this Directive. Member States may determine what constitutes serious damage according to their national law and practice, such as disrupting system services of significant public importance, or causing major financial cost or loss of personal data or sensitive information.***

(6) Large-scale cyber attacks can cause substantial economic damage both through the interruption of information systems and communication and through the loss or alteration of commercially important confidential information or other data. Particular attention should be paid to raising the awareness of innovative small and medium-sized enterprises to threats relating to such attacks and their vulnerabily to such attacks, due to their increased dependence on the proper functioning and availability of information systems and often limited resources for information security.

(7) Common definitions in this area are important in order to ensure a consistent approach in the Member States to the application of this Directive.

(8) There is a need to achieve a common approach to the constituent elements of criminal offences by introducing common offences of illegal access to an information system, illegal system interference, illegal data interference, and illegal interception.

(9) Interception includes, but is not necessarily limited to, the listening to, monitoring or surveillance of the content of communications and the procuring of the content of data either directly, through access and use of the information systems, or indirectly through the use of electronic eavesdropping or tapping devices by technical means.

(10) Member States should provide for penalties in respect of attacks against information systems. Those penalties should be effective, proportionate and dissuasive ***and should include imprisonment and/or fines***.

(11) This Directive provides for criminal penalties at least for cases which are not minor. Member States may determine what constitutes a minor case according to their national law and practice. A case may be considered minor, for example, where the damage caused by the offence and/or the risk to public or private interests, such as to the integrity of a computer system or to computer data, or to the integrity, rights or other interests of a person, is insignificant or is of such a nature that the imposition of a criminal penalty within the legal threshold or the imposition of criminal liability is not necessary.

(12) The identification and reporting of threats and risks posed by cyber attacks and the related vulnerability of information systems is a pertinent element of effective prevention of, and response to, cyber attacks and to improving the security of information systems. Providing incentives to report security gaps could add to that effect. Member States should endeavour to provide possibilities for the legal detection and reporting of security gaps.

(13) It is appropriate to provide for more severe penalties where an attack against an information system is committed by a criminal organisation, as defined in Council Framework Decision 2008/841/JHA of 24 October 2008 on the fight against organised crime[1]**,** where a cyber attack is conducted on a large scale, ***thus affecting a significant number of information systems, including where it is intended to create a botnet, or where a cyber attack causes serious damage, including where it is carried out through a botnet***. It is also appropriate to provide for more severe penalties where ▌ an attack ***is conducted against a critical infrastructure of the Member States or of the Union***.

(14) Setting up effective measures against identity theft and other identity-related offences constitutes another important element of an integrated approach against cybercrime. Any need for Union action against this type of criminal behaviour could also be considered in the context of evaluating the need for a comprehensive horizontal Union instrument.

(15) The Council Conclusions of 27 to 28 November 2008 indicated that a new strategy should be developed with the Member States and the Commission, taking into account the content of the 2001 Council of Europe Convention on Cybercrime. That Convention is the legal framework of reference for combating cybercrime, including attacks against information systems. This Directive builds on that Convention. ***Completing the process of ratification of that Convention by all Member States as soon as possible should be considered to be a priority.***

[1] OJ L 300, 11.11.2008, p. 42.

(16) Given the different ways in which attacks can be conducted, and given the rapid developments in hardware and software, this Directive ***refers*** to tools that can be used in order to commit the offences laid down in this Directive. Such tools could include malicious software, including ***those able to create*** botnets, used to commit cyber attacks. ***Even where such a tool is suitable or particularly suitable for carrying out one of the offences laid down in this Directive, it is possible that it was produced for a legitimate purpose Motivated by the need to avoid criminalisation where such tools are produced and put on the market for legitimate purposes, such as to test the reliability of information technology products or the security of information systems, apart from the general intent requirement, a direct intent requirement that those tools be used to commit one or more of the offences laid down in this Directive must be also fulfilled.***

(17) ***This Directive does not impose criminal liability where the objective criteria of the offences laid down in this Directive are met but the acts*** are committed without criminal intent, ***for instance where a person does not know that access was unauthorised or in the case of mandated testing or protection of information systems, such as where a person is assigned by a company or vendor to test the strength of its security system. In the context of this Directive, contractual obligations or agreements to restrict access to information systems by way of a user policy or terms of service, as well as labour disputes as regards the access to and use of information systems of an employer for private purposes, should not incur criminal liability where the access under such circumstances would be deemed unauthorised and thus would constitute the sole basis for criminal proceedings. This Directive is without prejudice to the right of access to information as laid down in national and Union law, while at the same time it may not serve as a justification for unlawful or arbitrary access to information.***

(18) Cyber attacks could be facilitated by various circumstances, such as where the offender has access to security systems inherent in the affected information systems within the scope of his or her employment. In the context of national law, such circumstances should be taken into account in the course of criminal proceedings as appropriate.

(19) Member States should provide for aggravating circumstances in their national law in accordance with the applicable rules established by their legal systems on aggravating circumstances. They should ensure that those aggravating circumstances are available for judges to consider when sentencing offenders. It remains within the discretion of the judge to assess those circumstances together with the other facts of the particular case.

(20) This Directive does not govern conditions for exercising jurisdiction over any of the offences referred to herein, such as a report by the victim in the place where the offence was commited, a denunciation from the State of the place where the offence was commited, or the non-prosecution of the offender in the place where the offence was committed.

(21) In the context of this Directive, States and public bodies remain fully bound to guarantee respect for human rights and fundamental freedoms, in accordance with existing international obligations.

(22) This Directive strengthens the importance of networks, such as the G8 or the Council of Europe's network of points of contact available on a twenty-four hour, seven-day-a-week basis***. Those points of contact should be able to deliver effective assistance thus, for example, facilitating the exchange of relevant information available and the provision of technical advice or legal information*** for the purpose of investigations or proceedings concerning criminal offences ***relating*** to information systems and ***associated data involving the requesting Member State. In order to ensure the smooth operation of the networks, each contact point should have the capacity to communicate with the point of contact of another Member State on an expedited basis with the support, inter alia, of trained and equipped personnel***. Given the speed with which large-scale ***cyber*** attacks can be carried out, Member States should be able to respond promptly to urgent requests from this network of contact points. ***In such cases, it may be expedient that the request for information be accompanied by telephone contact in order to ensure that the request is processed swiftly by the requested Member State and that feedback is provided within eight hours.***

(23) Cooperation between public authorities on the one hand, and the private sector and civil society on the other, is of great importance in preventing and combating attacks against information systems. It is necessary to foster and improve cooperation between service providers, producers, law enforcement bodies and judicial authorities, while fully respecting the rule of law. Such cooperation could include support by service providers in helping to preserve potential evidence, in providing elements helping to identify offenders and, as a last resort, in shutting down, completely or partially, in accordance with national law and practice, information systems or functions that have been compromised or used for illegal purposes. Member States should also consider setting up cooperation and partnership networks with service providers and producers for the exchange of information in relation to the offences within the scope of this Directive.

(24) There is a need to collect ***comparable*** data on the offences laid down in this Directive***. Relevant data should be made available to the competent specialised Union agencies and bodies, such as Europol and ENISA, in line with their tasks and information needs,*** in order to gain a more complete picture of the problem ***of cybercrime and network and information security*** at Union level and thereby to contribute to formulating a more effective response. ***Member States should submit information on the modus operandi of the offenders to Europol and its European Cybercrime Centre for the purpose of conducting threat assessments and strategic analyses of cybercrime in accordance with Council Decision 2009/371/JHA of 6 April 2009 establishing the European Police Office (Europol)[1]. Providing information can facilitate a better understanding of present and future threats and thus contribute to more appropriate and targeted decision-making on combating and preventing attacks against information systems.***

(25) The Commission should submit a report on the application of this Directive and make necessary legislative proposals which could lead to broadening its scope, taking into account developments in the field of cybercrime. Such developments could include technological developments, for example those enabling more effective enforcement in the area of attacks against information systems or facilitating prevention or minimising the impact of such attacks. For that purpose, the Commission should take into account the available analyses and reports produced by relevant actors and, in particular, Europol and ENISA.

[1] ***OJ L 121, 15.5.2009, p. 37.***

(26) In order to fight cybercrime effectively, it is necessary to increase the resilience of information systems by taking appropriate measures to protect them more effectively against cyber attacks. Member States should take the necessary measures to protect their critical infrastructure from cyber attacks, as part of which they should consider the protection of their information systems and associated data. Ensuring an adequate level of protection and security of information systems by legal persons, for example in connection with the provision of publicly available electronic communications services in accordance with existing Union legislation on privacy and electronic communication and data protection, forms an essential part of a comprehensive approach to effectively counteracting cybercrime. Appropriate levels of protection should be provided against reasonably identifiable threats and vulnerabilities in accordance with the state of the art for specific sectors and the specific data processing situations. The cost and burden of such protection should be proportionate to the likely damage a cyber attack would cause to those affected. Member States are encouraged to provide for relevant measures incurring liabilities in the context of their national law in cases where a legal person has clearly not provided an appropriate level of protection against cyber attacks.

(27) Significant gaps and differences in Member States' laws ***and criminal procedures*** in the area of attacks against information systems ▌ may hamper the fight against organised crime and terrorism, and may complicate effective police and judicial cooperation in this area. The transnational and borderless nature of modern information systems means that attacks against such systems have a ***cross-border*** dimension, thus underlining the urgent need for further action to approximate criminal law in this area. In addition, the coordination of prosecution of cases of attacks against information systems should be facilitated by the ***adequate implementation and application*** of Council Framework Decision 2009/948/JHA of 30 November 2009 on prevention and settlement of conflict of jurisdiction in criminal proceedings[1]. ***Member States, in cooperation with the Union, should also seek to improve international cooperation relating to the security of information systems, computer networks and computer data. Proper consideration of the security of data transfer and storage should be given in any international agreement involving data exchange.***

[1] OJ L 328, 15.12.2009, p. 42.

(28) Improved cooperation between the competent law enforcement bodies and judicial authorities across the Union is essential in an effective fight against cybercrime. In this context, stepping up the efforts to provide adequate training to the relevant authorities in order to raise the understanding of cybercrime and its impact, and to foster cooperation and the exchange of best practices, for example via the competent specialised Union agencies and bodies, should be encouraged. Such training should, inter alia, aim at raising awareness about the different national legal systems, the possible legal and technical challenges of criminal investigations, and the distribution of competences between the relevant national authorities.

(29) This Directive respects human rights and fundamental ***freedoms*** and observes the principles recognised in particular by the Charter of Fundamental Rights of the European Union ***and the European Convention for the Protection of Human Rights and Fundamental Freedoms***, including the protection of personal data***, the right to privacy***, freedom of expression and information, the right to a fair trial, the presumption of innocence and the rights of the defence, as well as the principles of legality and proportionality of criminal offences and penalties. In particular, this Directive seeks to ensure full respect for those rights and principles and must be implemented accordingly.

(30) The protection of personal data is a fundamental right in accordance with Article 16(1) TFEU and Article 8 of the Charter on Fundamental Rights of the European Union. Therefore, any processing of personal data in the context of the implementation of this Directive should fully comply with the relevant Union law on data protection.

(31) In accordance with Article 3 of the Protocol on the position of the United Kingdom and Ireland in respect of the Area of Freedom, Security and Justice, annexed to the Treaty on European Union and to the Treaty on the Functioning of the European Union, those Member States have notified their wish to take part in the adoption and application of this Directive [redacted].

(32) In accordance with Articles 1 and 2 of the Protocol on the position of Denmark annexed to the Treaty on European Union and to the Treaty on the Functioning of the European Union, Denmark is not taking part in the adoption of this Directive and is not bound by it or subject to its application.

(33) Since the objectives of this Directive, namely to subject attacks against information systems in all Member States to effective, proportionate and dissuasive criminal penalties and to improve and encourage cooperation between judicial and other competent authorities, cannot be sufficiently achieved by the Member States, and can therefore, by reason of their scale or effects, be better achieved at Union level, the Union may adopt measures in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportortionality, as set out in that Article, this Directive does not go beyond what is necessary in order to achieve those objectives.

(34) This Directive aims to amend and expand the provisions of Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems[1]. Since the amendments to be made are of substantial number and nature, Framework Decision 2005/222/JHA should, in the interests of clarity, be replaced in its entirety in relation to Member States participating in the adoption of this Directive,

HAVE ADOPTED THIS DIRECTIVE:

[1] ***OJ L 69, 16.3.2005, p. 67.***

Article 1
Subject matter

This Directive ***establishes minimum rules concerning the definition*** of criminal offences ***and sanctions*** in the area of attacks against information systems **–.** It also aims to ***facilitate the prevention of such offences*** and to improve cooperation ***between judicial and other competent authorities.***

Article 2
Definitions

For the purposes of this Directive, the following definitions shall apply:

(a) "information system" means a device or group of inter-connected or related devices, one or more of which, pursuant to a programme, automatically processes computer data, as well as computer data stored, processed, retrieved or transmitted by that device or group of devices for the purposes of its or their operation, use, protection and maintenance;

(b) "computer data" means a representation of facts, information or concepts in a form suitable for processing in an information system, including a programme suitable for causing an information system to perform a function;

(c) "legal person" means an entity having the status of legal person under the applicable law, but does not include States or public bodies acting in the exercise of State authority, or public international organisations;

(d) "without right" means conduct referred to in this Directive, including access***,*** interference***, or interception,*** which is not authorised by the owner or by another right holder of the system or of part of it, or not permitted under national law.

Article 3
Illegal access to information systems

Member States shall take the necessary measures to ensure that***, when committed intentionally, the*** access without right***,*** to the whole or to any part of an information system, is punishable as a criminal offence ***where committed by infringing a security measure***, at least for cases which are not minor.

Article 4
Illegal system interference

Member States shall take the necessary measures to ensure that ▌ seriously hinderingor interrupting the functioning of an information systemby inputting computer data, by transmitting, damaging, deleting, deteriorating, altering or suppressing such data, or by rendering such data inaccessible, ***intentionally*** and without right, is punishable as a criminal offence, at least for cases which are not minor.

Article 5
Illegal data interference

Member States shall take the necessary measures to ensure that ▌ deleting, damaging, deteriorating, altering or suppressing computer data on an information system, or rendering such data inaccessible, ***intentionally and without right,*** is punishable as a criminal offence, at least for cases which are not minor.

Article 6
Illegal interception

Member States shall take the necessary measures to ensure that ▌ intercepting, by technical means, non-public transmissions of computer data to, from or within an information system, including electromagnetic emissions from an information system carrying such computer data, intentionally and without right, is punishable as a criminal offence***, at least for cases which are not minor***.

Article 7
Tools used for committing offences

Member States shall take the necessary measures to ensure that the intentional production, sale, procurement for use, import, ▌ distribution or otherwise making available, of one of the following tools, without right and ~~or~~ with the intention that it be used to commit any of the offences referred to in Articles 3 to 6, is punishable as a criminal offence***, at least for cases which are not minor***:

(a) ▌ a computer programme, designed or adapted primarily for the purpose of committing any of the offences referred to in Articles 3 to 6;

(b) a computer password, access code, or similar data by which the whole or any part of an information system is capable of being accessed.

Article 8
Incitement, aiding ***and*** abetting and attempt

1. Member States shall ensure that the ***incitement***, or aiding and abetting, ***to commit*** an offence referred to in Articles 3 to 7 is punishable as a criminal offence.

2. Member States shall ensure that the attempt to commit ***an offence*** referred to in ***Articles 4 and 5*** is punishable as a criminal offence.

Article 9
Penalties

1. Member States shall take the necessary measures to ensure that the offences referred to in Articles 3 to 8 are punishable by effective, proportionate and dissuasive criminal penalties.

2. Member States shall take the necessary measures to ensure that the offences referred to in Articles 3 to 7 are punishable by a maximum term of imprisonment of at least two years***, at least for cases which are not minor***.

3. ***Member States shall take the necessary measures to ensure that the offences referred to in Articles 4 and 5, when committed intentionally, are punishable by a maximum term of imprisonment of at least three yearswherea significant number of information systems have been affected through the use of a tool, referred to in Article 7, designed or adapted primarily for that purpose.***

4. Member States shall take the necessary measures to ensure that offences referred to in Articles 4 and 5 are punishable by a maximum term of imprisonment of at least five years where:

(a) they are committed within the framework of a criminal organisation, as defined in Framework Decision 2008/841/JHA***, irrespective of the penalty provided for therein;***

(b) they cause serious damage; or

(c) they are committed against a critical infrastructure information system.

5. Member States shall take the necessary measures to ensure that when the offences referred to in Articles 4 and 5 are committed by misusing the personal data of another person, with the aim of gaining the trust of a third party, thereby causing prejudice to the rightful identity owner, this may, in accordance with national law, be regarded as aggravating circumstances, unless those circumstances are already covered by another offence, punishable under national law.

▌

Article 10
Liability of legal persons

1. Member States shall take the necessary measures to ensure that legal persons can be held liable for offences referred to in Articles 3 to 8, committed for their benefit by any person, acting either individually or as part of a body of the legal person, and having a leading position within the legal person, based on one of the following:

   (a) a power of representation of the legal person;

(b) an authority to take decisions on behalf of the legal person;

(c) an authority to exercise control within the legal person.

2. Member States shall take the necessary measures to ensure that legal persons can be held liable where the lack of supervision or control by a person referred to in paragraph 1 has allowed the commission, by a person under its authority, of any of the offences referred to in Articles 3 to 8 for the benefit of that legal person.

3. The liability of legal persons under paragraphs 1 and 2 shall not exclude criminal proceedings against natural persons who are perpetrators or ***inciters of***, or accessories to, any of the offences referred to in Articles 3 to 8.

Article 11
Sanctions against legal persons

1. Member States shall take the necessary measures to ensure that a legal person held liable pursuant to Article 10(1) is punishable by effective, proportionate and dissuasive sanctions, which shall include criminal or non-criminal fines and which may include other sanctions, such as:

(a) exclusion from entitlement to public benefits or aid;

(b) temporary or permanent disqualification from the practice of commercial activities;

(c) placing under judicial supervision;

(d) judicial winding-up;

(e) temporary or permanent closure of establishments which have been used for committing the offence.

2. Member States shall take the necessary measures to ensure that a legal person held liable pursuant to Article 10(2) is punishable by effective, proportionate and dissuasive sanctions or other measures.

Article 12
Jurisdiction

1. Member States shall establish their jurisdiction with regard to the offences referred to in Articles 3 to 8 where the offence has been committed:

(a) in whole or in part within their territory; or

(b) by one of their nationals***, at least in cases where the act is an offence where it was committed.***

2. When establishing jurisdiction in accordance with point (a) of paragraph 1, a Member State shall ensure that it has jurisdiction where:

(a) the offender commits the offence when physically present on its territory, whether or not the offence is against an information system on its territory; or

(b) the offence is against an information system on its territory, whether or not the offender commits the offence when physically present on its territory.

3. A Member State shall inform the Commission where it decides to establish jurisdiction over an offence referred to in Articles 3 to 8 committed outside its territory, including where:

(a) the offender has his or her habitual residence in its territory; or

(b) the offence is committed for the benefit of a legal person established in its territory.

Article 13
Exchange of information

1. For the purpose of exchanging information relating to the offences referred to in Articles 3 to 8, ▌ Member States shall ***ensure that they have an operational national point of contact*** and that they make use of the existing network of operational points of contact available 24 hours a day and seven days a week. Member States shall also ensure that they have procedures in place so ***that for urgent requests for assistance, the competent authority can indicate, within eight hours of receipt, at least whether the request will be answered, and the form and estimated time of such an answer***.

2. Member States shall inform the Commission of their appointed point of contact referred to in paragraph 1. The Commission shall forward that information to the other Member States ***and competent specialised Union agencies and bodies***.

3. Member States shall take the necessary measures to ensure that appropriate reporting channels are made available in order to facilitate the reporting of the offences referred to in Article 3 to 6 to the competent national authorities without undue delay.

Article 14
Monitoring and statistics

1. Member States shall ensure that a system is in place for the recording, production and provision of statistical data on the offences referred to in Articles 3 to ***7.***

2. The statistical data referred to in paragraph 1 shall, as a minimum, cover ***existing data on*** the number of offences referred to in Articles 3 to ***7 registered by*** the Member States***,*** and
- the number of persons prosecuted ***for*** and ***convicted of*** the offences referred to in Articles 3 to ***7.***

3. Member States shall transmit the data collected pursuant to this Article to the Commission. ***The Commission*** shall ▌ ensure that a consolidated review of the statistical reports is published ***and submitted to the competent specialised Union agencies and bodies***.

Article 15
Replacement of Framework Decision 2005/222/JHA

Framework Decision 2005/222/JHA is hereby ***replaced in relation to Member States participating in the adoption of this Directive***, without prejudice to the obligations of the Member States relating to the ***time limit*** for transposition ***of the Framework Decision*** into national law.

In relation to Member States participating in the adoption of this Directive, references to the Framework Decision ***2005/222/JHA*** shall be construed as references to this Directive.

Article 16
Transposition

1. Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive by …[*].▌ .

[*] ***OJ Please insert the date: two years after the date of entry into force of this Directive.***

2. Member States shall ***transmit*** to the Commission the text of the ***measures transposing into their national law the obligations imposed on them under this Directive.***

3. When Member States adopt ***those measures,*** they shall contain a reference to this Directive or shall be accompanied by such a reference on the occasion of their official publication***.*** ***The methods of making such a reference shall be laid down by the Member States.***

Article 17
Reporting

The Commission shall, by …*[*]*, submit a report to the European Parliament and the Council***,*** ***assessing the extent to which the Member States have taken the necessary measures in order to comply with this Directive, accompanied, if necessary, by legislative proposals. The Commission shall also take into account the technical and legal developments in the field of cybercrime, particularly with regard to the scope of this Directive***.

[*] ***OJ Please insert the date: four years after the date of entry into force of this Directive.***

Article 18
Entry into force

This Directive shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

Article 19
Addressees

This Directive is addressed to the Member States in accordance with the Treaties.

Done at ...,

For the European Parliament	*For the Council*
The President	*The President*